Claim Listing

1. (Currently Amended) A computer system, comprising:

a hard real-time operating system;

an application running under the hard real-time operating system; and

a security process running under the hard real-time operating system[[;]], wherein

the security process is configured to periodically, in hard real-time, check the integrity of the application and/or a data element used by the application and, if the integrity check of the application or the data element indicates that the application or data element has been tampered with, notify a user of the computer system and/or shut down at least part of the computer system or application, and

the security process includes a challenge handler that is configured to receive a challenge from an external monitor and provide a response thereto within a predetermined amount of time, wherein the external monitor is configured so that if the external monitor does not receive the response within a predetermined amount of time from sending the challenge, the external monitor notifies an administrator and/or shuts down at least part of the computer system or application.

2. (Original) In a computer system running a real-time operating system, a computer security method, comprising:

executing a security process under the real-time operating system, wherein the security process is

configured to periodically, in hard real-time, check the integrity of an application and/or a data element used by the application and notify a system administrator and/or shut down the application if the integrity check of the application or the data element indicates that the application or data element has been tampered with;

sending a challenge to the security process or to a challenge handler that monitors the integrity of the security process; and

notifying an administrator if a response to the challenge is not received within a predetermined amount of time.

3. (Original) A computer system, comprising:

a dual-kernel operating system comprising a real-time kernel and a non-real-time kernel;

a first real-time thread running under the real-time kernel, the first real-time thread being configured to monitor the integrity of an application running under the non-real-time kernel;

a second real-time thread running under the real-time kernel, the second real-time thread being configured to monitor integrity of the first real-time thread; and

a security process running under the non-real-time kernel, the security process being configured to check the integrity of the first real-time thread and/or the second real-time thread.

4. (New) The computer system of claim 1, wherein the integrity check performed by the security process includes

checking the execution scheduling of the application.

5. (New) The computer system of claim 4, wherein the security process is configured to raise an alarm if, after checking the execution scheduling of the application, the security process determines that the application is not being scheduled at a required minimum frequency.

6. (New) The computer system of claim 1, wherein the integrity check performed by the security process includes checking the integrity of the application's code.

7. (New) The computer system of claim 6, wherein the security process is configured to raise an alarm if, after checking the integrity of the application's code, the security process determines that the application code has been tampered with.

8. (New) The computer system of claim 1, wherein the external monitor is an application running on a second computer system that is connected to the first computer system.

9. (New) The computer system of claim 8, wherein the second computer system is connected to the first computer system by a network.

10. (New) The computer system of claim 9, wherein the network is a deterministic network.

11. (New) The computer system of claim 1, wherein the

external monitor includes a device of the computer system.

12. (New) The computer system of claim 11, wherein the device is a peripheral device.

13. (New) The computer system of claim 11, wherein the device is an on-chip security monitor.

14. (New) The computer system of claim 1, wherein the security process is further configured to update a data item with a sequence number indicating a number of cycles that have passed without detection of an intruder.

15. (New) The computer system of claim 14, wherein the security process is further configured to transmit the data item to the external monitor using an encryption key included in a challenge sent to the challenge handler.

16. (New) The computer system of claim 15, wherein the security process is further configured to transmit the data item to the external monitor within a predetermined amount of time from when the external monitor sent a challenge to the challenge handler.

17. (New) The method of claim 2, wherein the integrity check performed by the security process includes checking the execution scheduling of the application.

18. (New) The method of claim 17, further comprising the step of raising an alarm in response to the security process determining that the application is not being scheduled at a

required minimum frequency.

19. (New) The method of claim 2, wherein the integrity check performed by the security process includes checking the integrity of the application's code.

20. (New) The method of claim 19, further comprising the step of raising an alarm in response to the security process determining that the application's code has been tampered with.

21. (New) The method of claim 2, wherein the challenge is sent from an external monitor.

22. (New) The method of claim 21, wherein the external monitor is an application running on a second computer system that is connected to the first computer system.

23. (New) The method of claim 22, wherein the second computer system is connected to the first computer system by a deterministic network.

24. (New) The method of claim 2, further comprising the steps of receiving the challenge and transmitting the response in response to receiving the challenge.

25. (New) The method of claim 24, further comprising the step of sending an encryption key to the security process at or about the same time as sending the challenge to the security process.

26. (New) The method of claim 25, further comprising the steps of receiving the encryption key and encrypting the response using the encryption key prior to transmitting the response.

27. (New) The computer system of claim 3, wherein the first real-time thread is further configured to check a set of integrity markers of the non-real-time kernel.

28. (New) The computer system of claim 27, wherein the integrity markers include a checksum and/or digital signature of a data element that maintains information about a password file used by the non-real-time kernel.

29. (New) The computer system of claim 28, wherein the data element is an inode.

30. (New) The computer system of claim 28, wherein the application is programmed to encrypt and decrypt passwords stored in the password file.

31. (New) The computer system of claim 3, wherein the second real-time thread is further configured to check a set of integrity markers of the real-time kernel.

32. (New) The computer system of claim 3, further comprising a challenge handler executing under the real-time kernel.

33. (New) The computer system of claim 32, further comprising an external monitor.

34. (New) The computer system of claim 33, wherein the challenge handler is responsive to challenges sent from the external monitor to the challenge handler.

35. (New) The computer system of claim 34, wherein the challenge handler is configured to send a response to the external monitor in response to receiving from the external monitor a challenge.

36. (New) The computer system of claim 35, wherein the response includes an encrypted data item.

37. (New) The computer system of claim 35, wherein the external monitor is programmed to determine whether the response from the challenge handler was received by the external monitor within a predetermined amount of time.

38. (New) The computer system of claim 37, wherein the external monitor is further programmed to raise an alarm if it determines that the response from the challenge handler was not received by the external monitor within the predetermined amount of time.